DATE(S) ISSUED:

03/02/2011

SUBJECT: Multiple Vulnerabilities in Mozilla Products Could Allow Remote Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in the Mozilla Firefox, Mozilla Thunderbird and Mozilla SeaMonkey applications, which could allow remote code execution. Mozilla Firefox is a web browser used to access the Internet. Mozilla Thunderbird is an email client. Mozilla SeaMonkey is a cross platform Internet suite of tools ranging from a web browser to an email client. These vulnerabilities may be exploited if a user visits, or is redirected to a web page or opens a malicious file that is specifically designed to take advantage of these vulnerabilities. Successful exploitation of these vulnerabilities will result in either an attacker gaining the same privileges as the logged on user, or gaining session authentication credentials. Depending on the privileges associated with the user, an attacker could install programs; view, change, or delete data; or create new accounts with full user rights.

SYSTEMS AFFECTED:

• Mozilla Firefox 3.5.0 - 3.5.16

• Mozilla Firefox 3.6 - 3.6.13

• Mozilla Sea Monkey 2.0.1 - 2.0.11

• Mozilla Thunderbird 3.0.1 - 3.0.7

• Mozilla Thunderbird 3.1.1 - 3.1.7

RISK:

Government:

• Large and medium government entities: **High**

• Small government entities: **High**

Businesses:

• Large and medium business entities: **High**

• Small business entities: **High**

Home users: High

DESCRIPTION:
Multiple vulnerabilities have been discovered in Mozilla Firefox, Mozilla Thunderbird, and Mozilla Sea Monkey. Details of these vulnerabilities are as follows:

Miscellaneous memory safety hazards (rv:1.9.2.14/ 1.9.1.17) (MFSA 2011-01) Multiple memory corruption vulnerabilities in the browser engine affect Firefox, Thunderbird, and SeaMonkey. CVE-2011-0053, CVE-2011-0062

Recursive eval call causes confirm dialogs to evaluate to true (MFSA 2011-02) A security vulnerability regarding an eval() function call wrapped in a try/catch statement can leave the browser in an inconsistent state. An attacker may be able to exploit this issue to trick a user into accepting any dialog; other attacks may also be possible.This issue affects Firefox and SeaMonkey. CVE-2011-0051

Use-after-free error in JSON.stringify (MFSA 2011-03) A use-after-free error exists in a method used by JSON.stringify. An attacker may be able to exploit this issue to execute arbitrary code. This issue affects Firefox and SeaMonkey. CVE-2011-0055

Buffer overflow in JavaScript upvarMap (MFSA 2011-04) A buffer-overflow vulnerability affects the JavaScript engine's internal memory when mapping non-local JS variables. An attacker may be able to exploit this issue to execute arbitrary code. This issue affectsFirefox and SeaMonkey. CVE-2011-0054

Buffer overflow in JavaScript atom map(MFSA 2011-05) A buffer-overflow vulnerability affects the JavaScript engine's internal mapping of string values when handling error cases where the number of values is above 64K. An attacker may be able to exploit this issue to execute arbitrary code. This issue affects Firefox and SeaMonkey. CVE-2011-0056

Use-after-free error using Web Workers (MFSA 2011-06) A use-after-free error due to an issue where a JavaScript worker could keep a reference to an object freed during garbage collection. An attacker may be able to exploit this issue to execute arbitrary code. This issue affectsFirefox and SeaMonkey. CVE-2011-0057

Memory corruption during text run construction (Windows) (MFSA 2011-07) A memory corruption issue occurs when very long strings are constructed and inserted in an HTML document. An attacker may be able to exploit this issue to execute arbitrary code. This issue affects Firefox and SeaMonkey. CVE-2011-0058

ParanoidFragmentSink allows javascript: URLs in chrome documents (MFSA 2011-08) An issue with regards to the 'ParanoidFragmentSink' class may have unknown impact against extension code utilizing the class. This issue affects Firefox, Thunderbird, and SeaMonkey. CVE-2010-1585

Crash caused by corrupted JPEG image (MFSA 2011-09) A buffer-overflow vulnerability occurs when decoding a specially crafted JPEG image. An attacker may be able to exploit this issue to execute arbitrary code. This issue affects Firefox, Thunderbird, and SeaMonkey. CVE-2011-0061

CSRF risk with plugins and 307 redirects (MFSA 2011-10) A cross-site request forgery vulnerability occurs when plug-in initiated requests handle 307 redirect responses. An attacker may be able to exploit this issue to execute arbitrary commands in the context of an unsuspecting victim. This issue affects Firefox and SeaMonkey CVE-2011-0059

Exploitation may occur if a user visits or is redirected to a web page, or receives a specially crafted email, which is specifically crafted to take advantage ofthese vulnerabilities. When an unsuspecting user visits

the malicious site or views the email, the exploit will be triggered, resulting in various unwanted actions being taken in the context of the targeted application.

Successful exploitation of these vulnerabilities may result in either an attacker gaining the same privileges as the logged on user, or gaining session authentication credentials. Depending on the privileges associated with the user, an attacker could install programs; view, change, or delete data; or create new accounts with full user rights.

RECOMMENDATIONS:
The following actions should be taken:

• Upgrade vulnerable Mozilla products immediately after appropriate testing.

• Remind users not to download or openfiles from un-trusted websites.

• Remind users not to open e-mail attachments from unknown users or suspicious e-mails from trusted sources.

• Run all software as a non-privilegeduser (one without administrative privileges) to diminish the effects of a successful attack.

REFERENCES:

Mozilla:
http://www.mozilla.org/security/announce/2011/mfsa2011-01.html
http://www.mozilla.org/security/announce/2011/mfsa2011-02.html
http://www.mozilla.org/security/announce/2011/mfsa2011-03.html
http://www.mozilla.org/security/announce/2011/mfsa2011-04.html
http://www.mozilla.org/security/announce/2011/mfsa2011-05.html
http://www.mozilla.org/security/announce/2011/mfsa2011-06.html
http://www.mozilla.org/security/announce/2011/mfsa2011-07.html
http://www.mozilla.org/security/announce/2011/mfsa2011-08.html
http://www.mozilla.org/security/announce/2011/mfsa2011-09.html
http://www.mozilla.org/security/announce/2011/mfsa2011-10.html

Security Focus:

http://www.securityfocus.com/bid/46368

CVE:

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0053

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0062

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0052

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0055

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0054

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0056

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0057

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0058

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1585

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0061

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0059